

5

10 Verfahren zu Überprüfung der Sicherheit und Zuverlässigkeit  
softwarebasierter elektronischer Systeme

15 Die Erfindung betrifft ein Verfahren zur Überprüfung der  
Sicherheit und Zuverlässigkeit softwarebasierter  
elektronischer Systeme unter Verwendung einer  
Zuverlässigkeitsfunktion zur Überprüfung der geforderten  
Funktionen des Systems auf der Grundlage der hierfür  
20 notwendigen Hardware-Komponenten des Systems. Weiterhin  
betrifft die Erfindung Verwendungen dieses Verfahrens sowie  
ein Computerprogramm und Computerprogrammprodukt zur  
Implementierung des Verfahrens.

25 Stand der Technik

Zuverlässigkeits- und Sicherheitsanforderungen bspw. an  
Fahrzeugfunktionen ergeben sich aus den Kundenwünschen  
unter Berücksichtigung der technischen, gesetzlichen und  
30 finanziellen Randbedingungen. Zuverlässigkeitsanforderungen  
an Fahrzeugfunktionen werden beispielsweise in Form von  
kurzen Reparaturzeiten oder langen Serviceintervallen  
vorgegeben. Sicherheitsanforderungen legen dagegen das  
sichere Verhalten des Fahrzeugs im Falle von Ausfällen und

- Störungen von Komponenten des Fahrzeugs fest. Die an Fahrzeugfunktionen gestellten Zuverlässigkeits- und Sicherheitsanforderungen legen von Anfang an auch Anforderungen an die technische Realisierung und
- 5 Nachweispflichten fest. Eine der mächtigsten Maßnahmen zur Erhöhung der Sicherheit und Zuverlässigkeit ist Redundanz. Da zunehmend Fahrzeugfunktionen oder Teile von Fahrzeugfunktionen durch Software realisiert werden, haben systematische Methoden zur Zuverlässigkeits- und
- 10 Sicherheitsanalyse auch zunehmenden Einfluss auf die Software-Entwicklung für elektronische Steuergeräte, etwa auf die Realisierung der Überwachungs-, Diagnose- und Sicherheitskonzepte.
- 15 Für komplexe elektronische Systeme müssen die Aktivitäten zur Absicherung der Zuverlässigkeit und Sicherheit frühzeitig geplant und in den gesamten Projektplan integriert werden.
- 20 Unter dem Begriff „System“ soll im Rahmen vorliegender Anmeldung je nach Kontext das Folgende verstanden werden: Der zum Erreichen einer bestimmten Funktion notwendige kleinste Systemabschnitt, zusammenwirkende Systemabschnitte bis hin zum Gesamtsystem oder - noch weiter gefasst - das
- 25 Gesamtsystem unter Einschluss der Bedienpersonen oder anderer auf das Gesamtsystem wirkender Elemente. Zur Erläuterung der Erfindung wird im Rahmen vorliegender Anmeldung im Wesentlichen auf Systeme Bezug genommen, die Bestandteil von Fahrzeugsteuerungen sind. Diese Bezugnahme
- 30 hat rein erläuternden Charakter und soll die Erfindung in keiner Weise auf solche Systeme beschränken. Die Erfindung besitzt vielmehr generell in Bezug auf softwarebasierte elektronische Systeme Gültigkeit.

Zur Überprüfung der Sicherheit und Zuverlässigkeit solcher Systeme ist die Verwendung von Zuverlässigkeitsfunktionen bekannt, mit Hilfe derer der Grad der Zuverlässigkeit für geforderte Funktionen des Systems angegeben werden kann.

5 Zum Bestimmen einer solchen Zuverlässigkeitsfunktion kann von den Zuverlässigkeiten der für die geforderten Systemfunktionen notwendigen Hardwarekomponenten des Systems ausgegangen werden. Zuverlässigkeitsanalysen umfassen z.B. Ausfallraten- und Ausfallartenanalysen, wie

10 die Ausfallarten- und Wirkungsanalyse (FMIA) oder die Fehlerbaumanalyse (FTA). Im Folgenden soll eine Zuverlässigkeitsanalyse anhand einer Ausfallratenanalyse unter Berechnung der Zuverlässigkeitsfunktion anhand eines Zuverlässigkeitsblockdiagramms für ein betrachtetes System

15 näher erläutert werden.

Die systematische Untersuchung der Ausfallrate einer Betrachtungseinheit ermöglicht die Voraussage der Zuverlässigkeit für die Betrachtungseinheit durch

20 Berechnung. Diese Voraussage ist wichtig, um Schwachstellen frühzeitig zu erkennen, Alternativlösungen zu bewerten und Zusammenhänge zwischen Zuverlässigkeit, Sicherheit und Verfügbarkeit quantitativ erfassen zu können. Außerdem sind Untersuchungen dieser Art notwendig, um

25 Zuverlässigkeitsanforderungen etwa an Systemkomponenten stellen zu können.

Infolge von Vernachlässigungen und Vereinfachungen, sowie der Unsicherheit der verwendeten Eingangsdaten kann die

30 berechnete, vorausgesagte Zuverlässigkeit nur ein Schätzwert für die wahre Zuverlässigkeit sein, die nur mit Zuverlässigkeitsprüfungen und Feldbeobachtungen zu ermitteln ist. Im Rahmen von Vergleichsuntersuchungen in der Analysephase spielt jedoch die absolute Genauigkeit

keine Rolle, so dass besonders bei der Bewertung von Realisierungsalternativen die Berechnung der vorausgesagten Zuverlässigkeit nützlich ist.

- 5 In den folgenden Abschnitten ist die Betrachtungseinheit immer ein technisches System oder eine Systemkomponente des Fahrzeugs. Im allgemeinen Fall kann die Betrachtungseinheit auch weiter gefasst werden und beispielsweise auch den Fahrer des Fahrzeugs mit einschließen.

10

Die Ausfallratenanalyse (siehe hierzu Alessandro Birolini: Zuverlässigkeit von Geräten und Systemen. Springer Verlag, 1997) unterscheidet die folgenden Schritte:

- 15    ◦ Definition der Grenzen und Komponenten des technischen Systems, der geforderten Funktionen und des Anforderungsprofils
- Aufstellen des Zuverlässigkeitsblockdiagramms (engl. Reliability Block Diagram)
- 20    ◦ Bestimmung der Belastungsbedingungen für jede Komponente
- Bestimmung von Zuverlässigkeitsfunktion oder Ausfallrate für jede Komponente
- Berechnung der Zuverlässigkeitsfunktion für das System
- 25    ◦ Behebung der Schwachstellen

Die Ausfallratenanalyse ist ein mehrstufiges Verfahren und kann „top down“ von der Systemebene über die verschiedenen Subsystemebenen bis zur Komponentenebene der technischen Systemarchitektur durchgeführt werden. Die

30 Ausfallratenanalyse muss nach Änderungen der technischen Systemarchitektur wiederholt werden.

Im Folgenden soll der erste Schritt der Ausfallratenanalyse näher erläutert werden.

- Für die theoretischen Überlegungen, die zur Voraussage der  
5 Zuverlässigkeit notwendig sind, sollten eingehende  
Kenntnisse des Systems und seiner Funktionen, sowie der  
konkreten Möglichkeiten zur Verbesserung der  
Zuverlässigkeit und Sicherheit vorausgesetzt werden.  
Zum Systemverständnis zählt die Kenntnis der Architektur  
10 des Systems und seiner Wirkungsweise, die Arbeits- und  
Belastungsbedingungen für alle Systemkomponenten, sowie die  
gegenseitigen Wechselwirkungen zwischen den Komponenten,  
etwa in Form von Signalflüssen und der Eingangs- und  
Ausgangssicht aller Komponenten.  
15 Zu den Verbesserungsmöglichkeiten gehören die Begrenzung  
oder die Verringerung der Belastung der Komponenten im  
Betrieb, etwa der statischen oder dynamischen Belastungen,  
der Belastung der Schnittstellen, der Einsatz besser  
geeigneter Komponenten, die Vereinfachung des System- oder  
20 Komponentenentwurfs, die Vorbehandlung kritischer  
Komponenten, sowie der Einsatz von Redundanz.

Die geforderte Funktion spezifiziert die Aufgabe des  
Systems. Die Festlegung der Systemgrenzen und der  
25 geforderten Funktionen bildet den Ausgangspunkt jeder  
Zuverlässigkeitsanalyse, weil damit auch der Ausfall  
definiert wird.

Zusätzlich müssen die Umweltbedingungen für alle  
30 Komponenten des Systems definiert werden, da dadurch die  
Zuverlässigkeit der Komponenten beeinflusst wird. So hat z.  
B. der Temperaturbereich großen Einfluss auf die  
Ausfallrate von Hardware-Komponenten. Im Fahrzeug gehören  
z. B. der geforderte Temperaturbereich, der Einsatz unter

Feuchtigkeit, Staub oder korrosiver Atmosphäre, oder Belastungen durch Vibrationen, Schocks oder Schwankungen, wie etwa der Versorgungsspannung zu den Umweltbedingungen. Hängen die geforderten Funktionen und die Umweltbedingungen außerdem von der Zeit ab, muss ein Anforderungsprofil festgelegt werden. Ein Beispiel für gesetzlich vorgeschriebene Anforderungsprofile im Fahrzeug sind die Fahrzyklen zum Nachweis der Einhaltung der Abgasvorschriften. In diesem Fall spricht man auch von repräsentativen Anforderungsprofilen.

Nachstehend wird der zweite Schritt der Ausfallratenanalyse näher erläutert.

Das Zuverlässigkeitsblockdiagramm gibt Antwort auf die Fragen, welche Hardware-Komponenten eines Systems zur Erfüllung der geforderten Funktion grundsätzlich funktionieren müssen und welche Hardware-Komponenten im Falle ihres Ausfalls die Funktion nicht grundsätzlich beeinträchtigen, da sie redundant vorhanden sind. Die Aufstellung des Zuverlässigkeitsblockdiagramms erfolgt, indem man die Komponenten der technischen Systemarchitektur betrachtet. Diese Komponenten werden in einem Blockdiagramm so verbunden, dass die zur Funktionserfüllung notwendigen Komponenten in Reihe geschaltet werden und redundante Komponenten in einer Parallelschaltung verbunden werden.

Figur 1 stellt schematisch ein so genanntes Brake-By-Wire-System 1 dar, wobei das Bremspedal 2, das Steuergerät 3 sowie die vier Bremseinheiten, nämlich die Bremseinheit 4 vorne links, die Bremseinheit 5 hinten links, die Bremseinheit 6 vorne rechts sowie die Bremseinheit 7 hinten rechts, dargestellt sind. Die für eine Funktion des Systems 1 notwendigen Hardware-Komponenten sind mit K bezeichnet.

Für ein fiktives Brake-By-Wire-System 1, wie in Figur 1 dargestellt, wird zunächst die Systemgrenze festgelegt. Das System besteht aus den Komponenten Bremspedaleinheit ( $K_1$ ),  
5 Steuergerät ( $K_2$ ), den Radbremseinheiten ( $K_5, K_7, K_9, K_{11}$ ) und den elektrischen Verbindungen ( $K_3, K_4, K_6, K_8, K_{10}$ ).

Bei Brake-By-Wire-Systemen besteht zwischen dem Bremspedal und den Radbremsen keine hydraulische, sondern eine  
10 elektrische Verbindung. Beim Bremsen wird der Fahrerbefehl, der durch die Bremspedaleinheit  $K_1$  vorgegeben und im Steuergerät  $K_2$  verarbeitet wird, und die zum Bremsen notwendige Energie „by wire“ zu den Radbremseinheiten  $K_5, K_7, K_9$  und  $K_{11}$  übertragen. Dabei muss sichergestellt werden,  
15 dass die Übernahme der Funktionen „Informations- und Energieübertragung“ zwischen Pedaleinheit und Radbremseinheiten, die bei konventionellen Bremssystemen mechanisch-hydraulisch realisiert sind, durch die elektrischen und elektronischen Komponenten  $K_2, K_3, K_4, K_6, K_8$  und  $K_{10}$  kein zusätzliches Sicherheitsrisiko, sondern  
20 einen Sicherheitsgewinn bringt. Die vorhersagbare Übertragung der Bremsbefehle ist deshalb eine zwingende Voraussetzung. Ebenso muss die Sicherheit auch bei Störungen und Ausfällen von Komponenten gewährleistet sein.

25 Es soll die Funktion „Bremsen“ betrachtet werden. Dafür soll die Gesamtzuverlässigkeit des Systems bestimmt werden. Es wird angenommen, dass die Ausfallraten  $\lambda_1$  bis  $\lambda_{11}$  der Komponenten  $K_1$  bis  $K_{11}$  bekannt sind.

30 Dieses Beispiel wird im weiteren sehr stark vereinfacht. Es soll nur die prinzipielle Vorgehensweise bei der Zuverlässigkeitsanalyse verdeutlichen. Deshalb wird nur die Informationsübertragung betrachtet, während die Aspekte der

Energieversorgung und der Energieübertragung, sowie fahrdynamische Randbedingungen, wie die geforderte Bremskraftverteilung auf Vorder- und Hinterachse, die selbstverständlich auch bei der Zuverlässigkeitsanalyse  
5 berücksichtigt werden müssen, vernachlässigt werden.

Für die Erfüllung der Funktion „Bremsen“ sind bei dieser vereinfachten Sicht das Funktionieren der Komponenten Bremspedaleinheit  $K_1$ , Steuergerät  $K_2$ , sowie der  
10 Verbindungen zwischen Bremspedaleinheit und Steuergerät  $K_3$  zwingend notwendig.

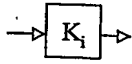
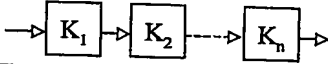
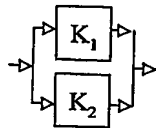
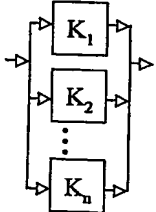
Bei den Radbremseinheiten und den Verbindungen zwischen Steuergerät und Radbremseinheiten ist Redundanz vorhanden.  
15 Unter der stark vereinfachten Annahme, dass eine ausreichende Hilfsbremswirkung für das Fahrzeug mit nur einer Radbremseinheit erzielt werden kann, sind dann beispielsweise die Komponenten  $K_4$  und  $K_5$  notwendig, während die Komponenten  $K_6$  und  $K_7$ ,  $K_8$  und  $K_9$  bzw.  $K_{10}$  und  $K_{11}$   
20 redundant vorhanden sind. Eine derartige Anordnung wird auch als 1-aus-4-Redundanz bezeichnet.

Das Zuverlässigkeitsblockdiagramm für die Funktion „Bremsen“ sieht dann wie in Figur 2 dargestellt aus.  
25

Nach Festlegung der Belastungsbedingungen und der Bestimmung der Zuverlässigkeitsfunktionen  $R_i(t)$  für alle Komponenten  $K_i$ , kann unter Berücksichtigung der in nachstehender Tabelle 3 dargestellten Grundregeln für  
30 Zuverlässigkeitsblockdiagramme die Zuverlässigkeitsfunktion des Systems  $R_s(t)$  berechnet werden.



Tabelle 3: Einige Grundregeln zur Berechnung der Zuverlässigkeitsfunktion für das System

Zuverlässigkeitsblockdiagramm	Zuverlässigkeitsfunktion $R_S = R_S(t), R_i = R_i(t)$	Ausfallrate $\lambda_S$ für $\lambda_i = \text{konstant}$ : $R_i(t) = e^{-\lambda_i t}$	Beispiel
	$R_S = R_1$	$\lambda_S = \lambda_1$	
	$R_S = \prod_{i=1}^n R_i$	$\lambda_S = \sum_{i=1}^n \lambda_i$	$R_1 = R_2 = 0,9$ $R_S = 0,9 \cdot 0,9 = 0,81$
 1-aus-2-Redundanz	$R_S = 1 - (1 - R_1)(1 - R_2)$ $= R_1 + R_2 - R_1 \cdot R_2$		$R_1 = R_2 = 0,9$ $R_S = 1 - (1 - 0,9)(1 - 0,9) = 0,99$
 k-aus-n-Redundanz	$R_1 = R_2 = \dots = R_n = R$ $R_S = \sum_{i=k}^n \binom{n}{i} R^i (1-R)^{n-i}$  Für $k=1$ gilt: $R_S = 1 - (1-R)^n$		$R_1 = R_2 = R_3 = R_4 = 0,9$ bei 1-aus-4-Redundanz: $R_S = 1 - (1 - 0,9)^4 = 0,9999$

5

Für das Beispiel in Figur 2 kann damit die Zuverlässigkeitsfunktion des Systems  $R_S$  berechnet werden. Mit den Annahmen  $R_4 = R_6 = R_8 = R_{10}$  und  $R_5 = R_7 = R_9 = R_{11}$  folgt für  $R_S$ :

10

$$R_S = R_1 R_2 R_3 [1 - (1 - R_4 R_5)^4]$$

Wie dieses vereinfachte Beispiel zeigt, erhöht sich die Systemzuverlässigkeit für eine Funktion durch redundante Komponenten im Zuverlässigkeitsblockdiagramm gegenüber der

15

- Komponentenzuverlässigkeit. Dagegen verringert sich bei den seriell dargestellten Komponenten die Systemzuverlässigkeit gegenüber der Komponentenzuverlässigkeit. Man wird daher für die seriellen Komponenten im
- 5 Zuverlässigkeitsblockdiagramm bereits eine hohe Zuverlässigkeit von den Komponenten fordern müssen oder eine technische Systemarchitektur einführen, die auch hier redundante Strukturen vorsieht.
- 10 Während oben die Berechnung der Zuverlässigkeitsfunktion für ein System für eine bestimmte geforderte Systemfunktion exemplarisch und stark vereinfacht dargelegt worden ist, ist es in ähnlicher Weise erstrebenswert, Aussagen über die Sicherheit eines Systems treffen zu können. Für die
- 15 Sicherheit eines Systems ist es häufig irrelevant, ob die Betrachtungseinheit die geforderten Funktionen erfüllt oder nicht, sofern damit kein nicht vertretbar hohes Risiko eintritt. Softwarebasierte elektronische Systeme, wie sie in vorliegender Anmeldung betrachtet werden, bestehen
- 20 hauptsächlich aus Hardware-Komponenten sowie Software-Komponenten, wobei die Software-Komponenten meist auf einige der Hardwarekomponenten des Systems verteilt sein können. Es besteht ein starkes Bedürfnis, sowohl die Sicherheit als auch die Zuverlässigkeit solcher
- 25 softwarebasierter elektronischer System verlässlich überprüfen zu können.

#### Beschreibung der Erfindung und Vorteile

- 30 Erfindungsgemäß wird eine Zuverlässigkeitsfunktion zur Berechnung der Zuverlässigkeit mindestens einer der geforderten Funktionen des Systems und eine weitere Zuverlässigkeitsfunktion zur Berechnung der Zuverlässigkeit mindestens einer der

Sicherheitsfunktionen des Systems bestimmt, wobei bei der Bestimmung dieser Zuverlässigkeitsfunktionen auch Software-Komponenten des Systems mit berücksichtigt werden. Die Software-Komponenten werden dabei anhand  
5 der Hardware-Komponenten, auf die diese Softwarekomponenten verteilt sind, mit berücksichtigt. Diese Berücksichtigung kann sich dabei auf die Hardware-Komponente(n) selbst sowie auch auf die entsprechenden Hardware-Verbindungen erstrecken, die  
10 von der jeweiligen Software-Komponente (z.B. durch Abgabe eines Ausgangssignals) beeinflusst werden. Hierdurch ist es erstmals möglich, Aussagen über die Sicherheit und Zuverlässigkeit eines softwarebasierten elektronischen Systems zu treffen, wobei diese Aussagen  
15 das aus Hardware- und Software-Komponenten einschließlich der jeweiligen Verbindungen bestehende System betreffen und sich nicht nur auf die Hardware-Komponenten beschränken.

20 Sicherheit und Zuverlässigkeit des Hardware- und Software-Komponenten umfassenden Systems werden unter Verwendung einer Zuverlässigkeitsfunktion überprüft, die bspw. anhand des eingangs erläuterten Zuverlässigkeitsblockdiagramms für das System bestimmt  
25 werden kann. Wie nachstehend erläutert wird, werden erfindungsgemäß die Software-Komponenten des Systems bei der Bestimmung der Zuverlässigkeitsfunktion mit berücksichtigt. Dies kommt einer neuen Systemdefinition gleich, da bisher für Zuverlässigkeitsanalysen nur ein  
30 aus Hardware-Komponenten bestehendes System betrachtet wurde und die Software-Komponenten - wenn überhaupt - einer eigenen gesonderten Analyse unterzogen wurden.

Mit der Erfindung ist die frühzeitige Bewertung unterschiedlicher Überwachungskonzepte elektronischer Steuergeräte im Besonderen und von Funktionen elektronischer Systeme im Allgemeinen, die durch Software und Hardware realisiert werden, hinsichtlich der erreichbaren Systemsicherheit und der Systemzuverlässigkeit möglich. Die Ergebnisse beeinflussen insbesondere die Verteilung von Software-Funktionen auf die Mikrocontroller vernetzter Steuergeräte und damit die Entwicklung von Software für verteilte und vernetzte Steuergeräte.

Um Aussagen über das System im Gesamten treffen zu können, ist es sinnvoll, alle Funktionen des Systems, also alle geforderten Systemfunktionen als auch alle Sicherheitsfunktionen des Systems mittels Bestimmung entsprechender Zuverlässigkeitsfunktionen zu überprüfen.

Zuverlässigkeitsfunktionen nehmen in der Regel einen bestimmten Wertebereich, bspw. von 0 bis 1, ein, wobei im Folgenden ohne Beschränkung der Allgemeingültigkeit davon ausgegangen werden soll, dass ein hoher Wert (1) für eine hohe, ein niedriger Wert (0) für eine niedrige Zuverlässigkeit stehen soll. Die erfindungsgemäßen Zuverlässigkeitsfunktionen beziehen sich zum einen auf die Zuverlässigkeit der geforderten Systemfunktionen, zum anderen auf die Zuverlässigkeit der Sicherheitsfunktionen des Systems. Nach der Bestimmung der entsprechenden Zuverlässigkeitsfunktionen ist es vorteilhaft, die konkreten Werte dieser Zuverlässigkeitsfunktionen für die gewählte Systemarchitektur (oder Systemkonfiguration) zu berechnen, um konkrete Aussagen über die

Zuverlässigkeit der Systemfunktionen bzw. der Sicherheitsfunktionen zu erhalten.

In der Regel sind neben der gewählten Systemarchitektur  
5 auch andere Konfigurationen realisierbar, die zu denselben geforderten Systemfunktionen führen. Gleiches gilt für die geforderten Sicherheitsfunktionen. Es ist daher für die Wahl einer geeigneten Systemarchitektur von Vorteil, wenn die erfindungsgemäß bestimmten  
10 Zuverlässigkeitsfunktionen für verschiedene Systemarchitekturen bestimmt werden. Die Systemarchitektur kann dabei wie folgt verändert werden: durch Festlegung der für die Realisierung der geforderten Systemfunktionen sowie  
15 Sicherheitsfunktionen notwendigen Hardware-Komponenten (Art der Hardware-Komponenten, Anordnung und Redundanzen dieser Komponenten); Festlegung der für die Realisierung der geforderten Systemfunktionen sowie Sicherheitsfunktionen notwendigen Softwarekomponenten  
20 und schließlich die Zuordnung der Softwarekomponenten zu bestimmten Hardwarekomponenten. Durch Variation einer oder mehrerer dieser Festlegungen bzw. Zuordnungen lässt sich die Systemarchitektur verändern.

25 Hierbei ist es sinnvoll, für die sich ergebenden Systemarchitekturen die Zuverlässigkeiten (Werte der Zuverlässigkeitsfunktionen) zu berechnen und Konfigurationen mit hoher Zuverlässigkeit den Vorzug zu geben. Die berechneten Zuverlässigkeiten können sich  
30 hierbei entweder auf die geforderten Systemfunktionen oder auf die Sicherheitsfunktionen des Systems beziehen. Es ist jedoch von Vorteil beide Zuverlässigkeiten zu maximieren, um eine Systemarchitektur zu finden, die sowohl hinsichtlich

Zuverlässigkeit als auch hinsichtlich Sicherheit hohe Werte erzielt.

5 Zur Erhöhung der Systemsicherheit ist es sinnvoll, die  
geforderten Systemfunktionen durch  
Überwachungsfunktionen zu kontrollieren. Hierdurch  
können rechtzeitig Maßnahmen ergriffen werden, falls  
eine bestimmte Systemfunktion vom System nicht mehr  
geliefert werden kann. Diese Maßnahmen reichen vom  
10 Abgeben einer entsprechenden Information bis hin zum  
Abschalten des gesamten Systems, um etwaige Risiken zu  
minimieren.

15 Die Sicherheit lässt sich weiter dadurch erhöhen, dass  
die Überwachungsfunktionen zur Überwachung der  
Systemfunktionen ihrerseits durch  
Systemüberwachungsfunktionen überwacht werden.

20 Weiterhin ist es von Vorteil, wenn die  
Systemüberwachungsfunktionen wenigstens zum Teil den  
Systemabschnitt überwachen, der die  
Überwachungsfunktionen zur Überwachung der  
Systemfunktionen enthält. Hierdurch lassen sich nicht  
nur die Überwachungsfunktionen, sondern der gesamte  
25 Systemabschnitt (bspw. Mikrocontroller) kontrollieren  
und ein Ausfall dieses Systemabschnitts detektieren.

Weiterhin ist von Vorteil, wenn die  
Systemüberwachungsfunktionen auf zwei Systemabschnitte  
30 verteilt werden, von denen ein Systemabschnitt die  
besagten Überwachungsfunktionen sowie die geforderten  
Systemfunktionen, die von diesen Überwachungsfunktionen  
kontrolliert werden, enthält. Eine solche Konfiguration  
ermöglicht nämlich die Überwachung der beiden

Systemabschnitte in jedwede Richtung, insbesondere eine gegenseitige Überwachung dieser Systemabschnitte.

Das erfindungsgemäße Verfahren lässt sich, wie im  
5 Folgenden näher erläutert wird, mit Vorteil dazu  
verwenden, in einem verteilten und vernetzten System  
(Steuergerät) Software-Komponenten zu Hardware-  
Komponenten (wie Mikrocontroller) optimal zuzuordnen.  
Weiterhin eignet sich das erfindungsgemäße Verfahren  
10 mit Vorteil zur Festlegung der Systemarchitektur eines  
softwarebasierten elektronischen Systems, insbesondere  
eines Steuergeräts, wie ein Motorsteuergerät.

Das erfindungsgemäße Verfahren lässt sich in der Praxis für  
15 die zumeist vorkommenden komplexen elektronischen Systeme  
zweckmäßig mittels eines Computerprogramms implementieren.  
Dieses Computerprogramm bestimmt die zugehörigen  
Zuverlässigkeitsfunktionen bei einer gegebenen  
Systemarchitektur und berechnet hieraus die entsprechenden  
20 Werte für die Zuverlässigkeit und Sicherheit des Systems.  
Bei Implementierung über ein Computerprogramm lässt sich  
insbesondere die Systemarchitektur effizient optimieren,  
wobei bekannte Optimierungsverfahren (wie Monte-Carlo-  
Verfahren) zum Einsatz kommen können. Bei Verwendung eines  
25 Zuverlässigkeitsblockdiagramms zur Bestimmung der  
Zuverlässigkeitsfunktion kann das Computerprogramm unter  
Verwendung der eingangs dargestellten Grundregeln  
(vergleiche Tabelle oben) schnell die entsprechende  
Zuverlässigkeitsfunktion ermitteln.

30

Das Computerprogramm kann auf geeigneten Datenträgern, wie  
EEPROMs, Flash-Memories, aber auch DVDs, CD-ROMs, Disketten  
oder Festplattenlaufwerken gespeichert sein. Auch das  
Herunterladen des Computerprogramms über interne oder

öffentlich nutzbare Netze (Intranet bzw. Internet) ist möglich.

#### Figurenbeschreibung

5

Figur 1 zeigt eine schematische Darstellung eines Brake-By-Wire-Systems als Beispiel eines elektronischen Systems;

10 Figur 2 zeigt das zum in Figur 1 dargestellten System zugehörige Zuverlässigkeitsblockdiagramm für die Funktion „Bremsen“;

15 Figur 3 zeigt das Beispiel einer Abfolge von Schritten bei der Zuverlässigkeits- und Sicherheitsanalyse und der Spezifikation zuverlässiger und sicherer Systeme;

20 Figur 4 zeigt schematisch Komponenten eines Steuergeräts als Beispiel eines verteilten und vernetzten Systems, das erfindungsgemäß hinsichtlich Sicherheit und Zuverlässigkeit überwacht wird;

25 Figur 5 zeigt verschiedene Zuverlässigkeitsblockdiagramme für Funktionen des in Figur 4 dargestellten Systems.

#### Beschreibung der bevorzugten Ausführungsformen

30 Die Figuren 1 und 2 wurden in der Beschreibungseinleitung bereits ausführlich behandelt.

Zunächst sollen anhand der Darstellung in Figur 3 die Schritte einer Zuverlässigkeits- und Sicherheitsanalyse



dargelegt werden. Es handelt sich dabei um iterative und zusammenhängende Prozesse mit mehreren Schritten. Sie haben Einfluss auf Anforderungen an die Hardware, Software und den Software-Entwicklungsprozess für elektronische Systeme.

5 Auch für die Sicherheitsanalyse eines Systems werden hier Methoden zur Ausfallartenanalyse, wie FMEA oder FTA, eingesetzt. Die Ausfallartenanalyse liefert eine Bewertung des Risikos für alle Funktionen des Systems.

Das zulässige Grenzrisiko wird in der Regel durch

10 sicherheitstechnische Festlegungen, wie Gesetze, Normen oder Verordnungen, implizit vorgegeben. Aus dem ermittelten Risiko für die Funktionen des Systems und dem zulässigen Grenzrisiko werden dann - beispielsweise anhand von Normen wie der IEC 61508 - sicherheitstechnische Anforderungen an

15 das System abgeleitet, die oft großen Einfluss auf den System-, den Hardware- und Software-Entwurf in der Elektronikentwicklung haben.

Für die durch die Ausfallartenanalyse bestimmten und

20 abgegrenzten, so genannten sicherheitsrelevanten Funktionen des Systems müssen besondere Schutzmaßnahmen getroffen werden, die beispielsweise in Hardware und Software realisiert werden können.

25 Im einzelnen zeigt Figur 3 zwei Hauptblöcke 9 und 10, wobei der erste Hauptblock 9 die Zuverlässigkeits- und Sicherheitsanalyse, der zweite Hauptblock 10 die Spezifikation zuverlässiger und sicherer Systeme betrifft.

In die Zuverlässigkeits- und Sicherheitsanalyse (Hauptblock

30 9) geht zum einen die logische Systemarchitektur 11 als auch zum anderen die technische Systemarchitektur 12 ein. Die technische Systemarchitektur 12 ist ihrerseits ein Ergebnis der Systemspezifikation, wobei eine geänderte

Systemspezifikation (Systemarchitektur) eine erneute Zuverlässigkeits- und Sicherheitsanalyse bedingt.

Am Anfang der Zuverlässigkeits- und Sicherheitsanalyse  
5 steht zum einen die Gefahrenanalyse 13, zum anderen die Identifikation relevanter Komponenten und Subsysteme (mit 14 bezeichneter Block). Aus der Gefahrenanalyse 13 ergeben sich die konkreten gefährlichen Situationen 15 und damit verbunden die Risiko-Ausfallarten- und Ausfallratenanalyse  
10 17, wie sie eingangs in der Beschreibungseinleitung ausführlich geschildert wurde. Ergebnis dieser Analyse 17 sind die Zuverlässigkeits- und Sicherheitsanforderungen 18 an das System. Auf der anderen Seite ergibt sich als Ergebnis der Identifikation 14 relevanter Komponenten und  
15 Subsysteme die zuverlässigkeits- und sicherheitsrelevanten Komponenten und Subsysteme 16 des Systems.

Aus den beiden Ergebnissen der Zuverlässigkeits- und Sicherheitsanalyse, nämlich die zuverlässigkeits- und  
20 sicherheitsrelevanten Komponenten und Subsysteme 16 sowie die Zuverlässigkeits- und Sicherheitsanforderungen 18 an das System, wird eine notwendige und mögliche Systemspezifikation (Hauptblock 10) abgeleitet. Die relevanten Komponenten und Subsysteme beeinflussen die  
25 Definition 19 des Verifikations- und Validationsprozesses sowie die Definition 20 der Anforderungen an technische Komponenten und Subsysteme. Die Zuverlässigkeits- und Sicherheitsanforderungen 18 an das System beeinflussen die Definition des Softwareentwicklungsprozesses (Block 21).

30

Konkrete Ergebnisse sind hier der Verifikations- und Validationsprozess 22, die Zuverlässigkeits- und Sicherheitsanforderungen 23 an die Hardware, die Zuverlässigkeits- und Sicherheitsanforderungen 24 an die

Software sowie der eigentliche Software-Entwicklungsprozess  
25.

5 Diese vier Ergebnisse führen zum Gesamtergebnis der  
technischen Systemarchitektur 12. Diese technische  
Systemarchitektur kann unter Umständen korrigiert werden  
und die genannten Schritte daraufhin wiederholt werden, um  
zu überprüfen, ob die geänderte Systemarchitektur zu einem  
System höherer Zuverlässigkeit und Sicherheit führt.

10 Der Nachweis der Sicherheit und Zuverlässigkeit dieser  
Überwachungskonzepte ist Voraussetzung für die Zulassung  
von Fahrzeugen zum Straßenverkehr. Im folgenden wird am  
Beispiel des Überwachungskonzeptes für ein E-Gas-System das  
15 Verfahren zur Beurteilung der Zuverlässigkeit und  
Sicherheit des Überwachungskonzeptes unter Einsatz von  
Zuverlässigkeitsblockdiagrammen dargestellt.

20 Als mögliche Gefahr für ein E-Gas-System wird ungewolltes  
Gasgeben und ein daraus folgender Unfall angenommen. Für  
das Motorsteuergerät bedeutet dies, dass alle diejenigen  
Steuerungs- und Regelungsfunktionen  $f_n$  sicherheitsrelevant  
sind, die zu einer unbeabsichtigten Erhöhung des  
Motordrehmoments führen können. Für diese Funktionen ist  
25 deshalb ein Überwachungskonzept notwendig.

In diesem Beispiel soll das etwas vereinfachte  
Überwachungskonzept, wie es seit Jahren in  
Motorsteuergeräten eingesetzt wird, bezüglich der  
30 Sicherheit und Zuverlässigkeit anhand des erfindungsgemäßen  
Verfahrens untersucht werden. Im Rahmen des Arbeitskreises  
„E-Gas“ des Verbandes der Automobilindustrie (VDA) wird  
dieses von der Robert Bosch GmbH entwickelte Basiskonzept  
derzeit zu einem standardisierten Überwachungskonzept für

Motorsteuerungen von Otto- und Dieselmotoren weiterentwickelt.

In Figur 4 ist das Überwachungskonzept für sicherheitsrelevante Steuerungs- und Regelungsfunktionen  $f_n$  dargestellt.

In Figur 4 ist als softwarebasiertes elektronisches System ein Steuergerät 30 dargestellt. Ein erster Mikrocontroller 31 dient als Funktionsrechner, während ein zweiter Mikrocontroller 32 als Überwachungsrechner eingesetzt wird. Signale gelangen in die Eingangsstufe 33 des Steuergeräts 30 und werden von dort dem A/D-Wandler 34 im Mikrocontroller 31 zugeführt. Das digitalisierte Signal löst die eigentlichen Steuerungs- und Regelungsfunktionen  $f_n$  (Block 41) aus. Parallel werden die Signale dem Block 42 zugeführt, der die Funktionen zur Überwachung der Steuerungs- und Regelungsfunktionen  $f_{0n}$  enthält. Zur Überwachung der Steuerungs- und Regelungsfunktionen ist der Block 41 mit dem Block 42 verbunden. Die genannten Überwachungsfunktionen  $f_{0n}$  werden ihrerseits von Funktionen zur Überwachung der Mikrocontroller, d. h. den so genannten Systemüberwachungsfunktionen, überprüft. Hierzu ist der Block 42 mit dem Block 43 verbunden. Die Blöcke 41, 42 und 43 sind Bestandteil der Software 45 des Mikrocontrollers 31. Die Blöcke 42 und 43 haben reine Überwachungsfunktionen.

Weiterhin in Figur 4 dargestellt ist der als Überwachungsrechner dienende Mikrocontroller 32, zu dessen Software 46 die Funktionen zur Überwachung der Mikrocontroller (Block 44) gehören. Hieraus ist ersichtlich, dass diese Funktionen zur Überwachung der Mikrocontroller (Systemüberwachungsfunktionen) auf die

beiden Mikrocontroller 31 und 32 verteilt sind. Hierauf wird später eingegangen. Die Blöcke 42, 43 und 44 repräsentieren die Überwachungsfunktionen 29.

5 Die vom Steuergerät ausgeführten Steuerungs- und  
Regelungsfunktionen  $f_n$  (Block 41) werden in Form eines  
Ausgangssignales an einen D/A-Wandler 35 gelegt, dessen  
Ausgang an der Endstufe 40 liegt. Die Ausgänge 36, 37 und  
38 der die Überwachung wahrnehmenden Blöcke 42, 43 bzw. 44  
10 werden einem Addierglied 39 zugeführt, so dass das Erkennen  
eines Fehlers durch einen der drei Blöcke 42, 43 oder 44 zu  
einem entsprechenden Ausgangssignal des Addiergliedes 39  
führt. Letzteres ist mit der Endstufe 40 verbunden, wodurch  
je nach Art des Fehlers auf die Endstufe definiert Einfluss  
15 genommen werden kann.

Im Folgenden soll auf die Funktion des in Figur 4  
dargestellten Überwachungskonzepts näher eingegangen  
werden.

20 Die sicherheitsrelevanten Steuerungs- und  
Regelungsfunktionen  $f_n$  werden durch die  
Überwachungsfunktionen  $f_{0n}$  ständig überwacht. Die  
Überwachungsfunktionen  $f_{0n}$  verwenden die gleichen  
25 Eingangsgrößen wie die Steuerungs- und Regelungsfunktionen  
 $f_n$ , arbeiten aber mit unterschiedlichen Daten und mit  
unterschiedlichen Algorithmen.

Die Funktionen zur Überwachung der Mikrocontroller  
30 (=Systemüberwachungsfunktionen) prüfen neben RAM-, ROM- und  
Mikroprozessorfunktionen beispielsweise auch, ob die  
Steuerungs- und Regelungsfunktionen  $f_n$  und die  
Überwachungsfunktionen  $f_{0n}$  überhaupt ausgeführt werden.  
Dies macht in diesem Beispiel den Einsatz eines zweiten

Mikrocontrollern 32 im Motorsteuergerät 30, eines so genannten Überwachungsrechners, notwendig. Die Funktionen zur Überwachung der Mikrocontroller 31, 32 werden auf den Funktionsrechner und den Überwachungsrechner verteilt.

- 5 Beide überwachen sich bevorzugt in einem Frage-Antwort-Spiel gegenseitig.

Als sicherer Zustand ist in diesem Ausführungsbeispiel die Stromabschaltung für die elektromechanische Drosselklappe festgelegt. Die Drosselklappe ist so konstruiert, dass sie nach einer Stromabschaltung selbsttätig die Leerlaufposition einnimmt. Der Übergang in den sicheren Zustand kann deshalb dadurch eingeleitet werden, dass eine Abschaltung der Endstufen 40 des Steuergeräts, die die Drosselklappe ansteuern, erfolgt. Der Motor kann so im Notlauf weiterbetrieben werden.

Sowohl die Überwachungsfunktionen  $f_{0n}$ , als auch die Funktionen zur Überwachung der Mikrocontroller auf dem Funktions- und auf dem Überwachungsrechner können also die Drosselklappenendstufen des Steuergeräts 30 abschalten. Im Falle eines erkannten Fehlers wird neben dieser Sicherheitsreaktion auch ein Eintrag im Fehlerspeicher vorgenommen. Außerdem wird meist auch eine Information an den Fahrer etwa über eine Anzeige im Kombiinstrument ausgegeben.

Soll die Zuverlässigkeit dieses Überwachungskonzepts beurteilt werden, so sind zunächst drei Arten von Funktionen zu unterscheiden:

- die Steuerungs- und Regelungsfunktionen  $f_n$
- die Überwachungsfunktionen  $f_{0n}$

- die Funktionen zur Überwachung der Mikrocontroller (=Systemüberwachungsfunktionen)

Die Zuverlässigkeitsblockdiagramme 45, 46, 47 für diese verschiedenen Funktionen lassen sich dann recht einfach  
5 bestimmen und sind in Figur 5 dargestellt.

Um die Systemzuverlässigkeit zu bestimmen, wird man alle drei Arten von Funktionen gleichzeitig fordern. Dann ergibt sich die Systemzuverlässigkeit durch eine Reihenschaltung  
10 dieser Blockdiagramme. Zusätzlich müssen auch die Komponenten  $K_7$  und  $K_8$  (Verbindung der Blöcke 43 und 44 in Fig. 4), die in den Blockdiagrammen der einzelnen Funktionen nicht vorkommen, in Reihe geschaltet werden.

15 Die Systemzuverlässigkeit  $R_s$  zuverlässigkeit ergibt sich durch Multiplikation der Zuverlässigkeit der drei Funktionen  $R_x$ ,  $x = A, B, C$  mit der Zuverlässigkeit der Komponenten  $K_7$ ,  $R_D$  und  $K_8$ ,  $R_E$  und ist wegen  $R_x < 1$  in jedem Fall geringer als die jeweilige Zuverlässigkeit der Funktionen  $R_x$ . Bei der  
20 Berechnung der Systemzuverlässigkeit müssen die Regeln für das Rechnen mit mehrfach auftretenden Elementen im Zuverlässigkeitsblockdiagrammen beachtet werden (vgl. Alessandro Birolini: Zuverlässigkeit von Geräten und Systemen, Anmerkungen oben).

25

$$R_s \text{ zuverlässigkeit} = R_A R_B R_C R_D R_E$$

Dagegen ist für die Sicherheit lediglich das zuverlässige Erkennen eines Ausfalls und der zuverlässige Übergang in  
30 den sicheren Zustand notwendig. Die Zuverlässigkeit  $R_s$  sicherheit dieser Sicherheitsreaktion wird durch die Zuverlässigkeit der Überwachungsfunktionen  $f_{0n}$  oder der Funktionen zur Überwachung der Mikrocontroller vorgegeben und ist deshalb höher als die Zuverlässigkeit der

Funktionen  $R_X$ . Zudem geht die Zuverlässigkeit der Komponenten  $K_7$ ,  $R_D$  und  $K_8$ ,  $R_E$  in die Berechnung von  $R_S$  Sicherheit nicht ein.

- 5 Die Zuverlässigkeitsfunktion für die Zuverlässigkeit der Sicherheitsfunktion (-reaktion) ist wie folgt:

$$R_S \text{ Sicherheit} = 1 - (1 - R_B)(1 - R_C)$$

- 10 Wie dieses Beispiel zeigt, können Maßnahmen zur Erhöhung der Sicherheit die Zuverlässigkeit des Systems verringern. Außerdem ist ersichtlich, dass Maßnahmen zur Erhöhung der Zuverlässigkeit zu einer Reduzierung der Sicherheit eines Systems führen können.

15

- Obwohl beim erfindungsgemäßen Verfahren im Grunde nur Hardware-Komponenten und -Verbindungen betrachtet werden, haben die Zuverlässigkeits- und Sicherheitsanalysen großen Einfluss auf die Software-Entwicklung. Wie am Beispiel der
- 20 Bewertung des Überwachungskonzeptes gezeigt, beeinflussen sie etwa die Zuordnung der Software-Funktionen zu den Mikrocontrollern in einem verteilten und vernetzten System oder die notwendigen Qualitätssicherungsmaßnahmen in der Software-Entwicklung. Dies ist gegenüber dem Stand der
- 25 Technik ein enormer Fortschritt und führt zu großen Vorteilen bei der Systementwicklung.

- Das erfindungsgemäße Verfahren ermöglicht die folgende Vorgehensweise zur Überprüfung der Sicherheit und
- 30 Zuverlässigkeit softwarebasierter elektronischer Systeme (vgl. Figuren 4 und 5):



- Schritt 1: Festlegung des Hardware-Netzwerks des elektronischen Systems, d. h. insbesondere Spezifikation der Mikrocontroller 31, 32 und ihrer Vernetzung;
- Schritt 2: Festlegung der Software-Komponenten 41 - 44,  
5 die für die Realisierung der Funktionen des elektronischen Systems erforderlich sind und Spezifikation der Kommunikation zwischen den Software-Komponenten 41 - 44;
- Schritt 3: Zuordnung der Software-Komponenten 41 - 44 zu den Mikrocontrollern 31, 32 des Hardware-Netzwerks;
- 10 Schritt 4: Aufstellen der Zuverlässigkeitsblockdiagramme 45 - 47 für die geforderten Funktionen des elektronischen Systems 30 ausgehend von den Hardware-Komponenten und Hardware-Verbindungen  $K_i$ ,  $i=1, \dots, 13$ ;
- 15 Schritt 5: Nachweis der Sicherheit und Zuverlässigkeit durch Berechnung der Zuverlässigkeit für die Sicherheitsfunktionen und der Zuverlässigkeit für die gesamten geforderten Funktionen des elektronischen Systems (30);
- 20 Schritt 6: ggf. Wiederholung der Schritte 1 bis 5 und Korrektur der Systemarchitektur, d. h. des Software- und Hardware-Netzwerks, sowie der Zuordnung der Software-Komponenten zu Hardware-Komponenten.

5

## Ansprüche

- 10 1. Verfahren zur Überprüfung der Sicherheit und  
Zuverlässigkeit softwarebasierter elektronischer Systeme  
unter Verwendung einer Zuverlässigkeitsfunktion zur  
Überprüfung der geforderten Funktionen des Systems (30) auf  
der Grundlage der hierfür notwendigen Hardwarekomponenten  
15 des Systems (30),

d a d u r c h g e k e n n z e i c h n e t, d a s s

- eine Zuverlässigkeitsfunktion zur Berechnung der  
20 Zuverlässigkeit mindestens einer der geforderten Funktionen  
des Systems (30) und eine weitere Zuverlässigkeitsfunktion  
zur Berechnung der Zuverlässigkeit mindestens einer der  
Sicherheitsfunktionen des Systems (30) bestimmt werden,  
wobei zur Bestimmung dieser Zuverlässigkeitsfunktionen  
25 Software-Komponenten (41, 42, 43, 44) des Systems anhand  
der Hardware-Komponenten, auf die diese Software-  
Komponenten (41, 42, 43, 44) verteilt sind,  
mitberücksichtigt werden.

- 30 2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,  
dass eine Zuverlässigkeitsfunktion für alle geforderten  
Funktionen des Systems (30) bestimmt wird.

3. Verfahren nach Anspruch 1 oder 2 , dadurch gekennzeichnet, dass eine Zuverlässigkeitsfunktion für alle Sicherheitsfunktionen des Systems (30) bestimmt wird.
- 5 4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Werte der beiden Zuverlässigkeitsfunktionen für eine bestimmte Systemarchitektur berechnet werden.
- 10 5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Systemarchitektur durch eine oder mehrere der folgenden Bestandteile verändert wird: Festlegung der für die Realisierung der geforderten Systemfunktionen und Sicherheitsfunktionen notwendigen Hardware-Komponenten;
- 15 Festlegung der für die Realisierung der geforderten Systemfunktionen und Sicherheitsfunktionen notwendigen Software-Komponenten; und die Zuordnung der Software-Komponenten zu Hardware-Komponenten.
- 20 6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass die Systemarchitektur anhand einer Maximierung der berechneten Zuverlässigkeiten für die geforderten Systemfunktionen bei unterschiedlichen Systemarchitekturen optimiert wird.
- 25 7. Verfahren nach Anspruch 4, 5 oder 6, dadurch gekennzeichnet, dass die Systemarchitektur anhand einer Maximierung der berechneten Zuverlässigkeiten für die Sicherheitsfunktionen des Systems bei verschiedenen
- 30 Systemarchitekturen optimiert wird.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass eine Zuverlässigkeitsfunktion mittels eines Zuverlässigkeitsblockdiagramms bestimmt wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die geforderten Systemfunktionen durch Überwachungsfunktionen zur Überwachung dieser
- 5 Systemfunktionen überwacht werden, wobei die Überwachungsfunktionen ihrerseits durch Systemüberwachungsfunktionen überwacht werden.
10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass die Systemüberwachungsfunktionen wenigstens zum Teil den Systemabschnitt (31) überwachen, der die Überwachungsfunktionen zur Überwachung der Systemfunktionen enthält.
- 15 11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Systemüberwachungsfunktionen auf zwei Systemabschnitte (31, 32) verteilt werden, von denen ein Systemabschnitt (31) die geforderten Systemfunktionen sowie deren Überwachungsfunktionen enthält.
- 20 12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass beide Systemabschnitte (31, 32) sich gegenseitig über die Systemüberwachungsfunktionen überwachen.
- 25 13. Verfahren nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass zur Überprüfung der Sicherheit und Zuverlässigkeit des Systems (30) folgende Schritte ausgeführt werden:
- 30        Festlegung von Hardware-Komponenten des Systems (30) und deren Vernetzung, insbesondere Spezifikation der Mikrocontroller (31, 32) und ihrer Vernetzung;
- Festlegung von Software-Komponenten (41, 42, 43, 44) des Systems (30), die für die Realisierung der Systemfunktionen und der Sicherheitsfunktionen des Systems

(30) erforderlich sind und Spezifikation der Kommunikation zwischen den Software-Komponenten (41, 42, 43, 44);

Zuordnung der Software-Komponenten (41, 42, 43, 44) zu Hardware-Komponenten, insbesondere zu den Mikrocontrollern  
5 (31, 32) des Systems (30);

Aufstellen der Zuverlässigkeitsblockdiagramme (45, 46, 47) für die geforderten Funktionen des Systems (30) einschließlich der Sicherheitsfunktionen ausgehend von den Hardware-Komponenten und Hardware-Verbindungen;

10 Berechnung der Zuverlässigkeit für die Sicherheitsfunktionen und der Zuverlässigkeit für die gesamten geforderten Funktionen des Systems (30) zum Nachweis der Sicherheit und Zuverlässigkeit des Systems (30).

15

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass als weiterer Schritt die Systemarchitektur, also das Software- und Hardware-Netzwerk sowie die Zuordnung der Software-Komponenten zu Hardware-Komponenten, korrigiert  
20 wird und die Schritte gemäß Anspruch 13 wiederholt werden.

15. Verwendung eines Verfahrens nach einem der Ansprüche 1 bis 14 zur Zuordnung der Software-Komponenten (41, 42, 43, 44) zu Hardware-Komponenten, wie Mikrocontroller (31, 32),  
25 in einem verteilten und vernetzten System (30).

16. Verwendung eines Verfahrens nach einem der Ansprüche 1 bis 14 zur Festlegung der Systemarchitektur eines Steuergeräts (30), wie Motorsteuergerät.

30

17. Computerprogramm mit Programmcode-Mitteln, um alle Schritte eines Verfahrens gemäß einem der Ansprüche 1 bis 14 durchzuführen, wenn das Computerprogramm auf einem

Computer oder einer entsprechenden Rechneinheit ausgeführt wird.

18. Computerprogrammprodukt mit Programmcode-Mitteln, die  
5 auf einem computerlesbaren Datenträger gespeichert sind, um  
alle Schritte eines Verfahrens nach einem der Ansprüche 1  
bis 14 durchzuführen, wenn das Computerprogrammprodukt auf  
einem Computer oder auf einer entsprechenden Rechneinheit  
ausgeführt wird.

1/4

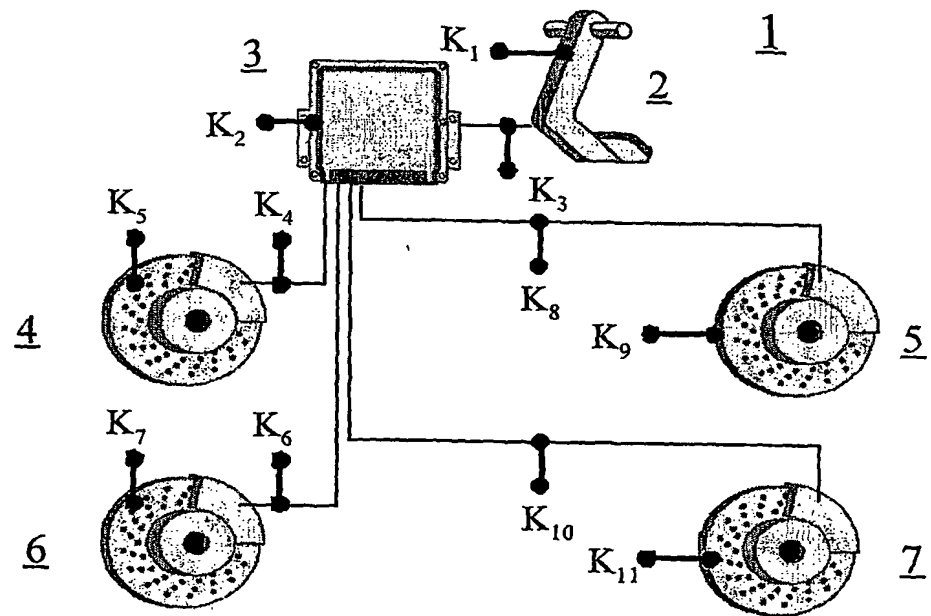


Fig. 1

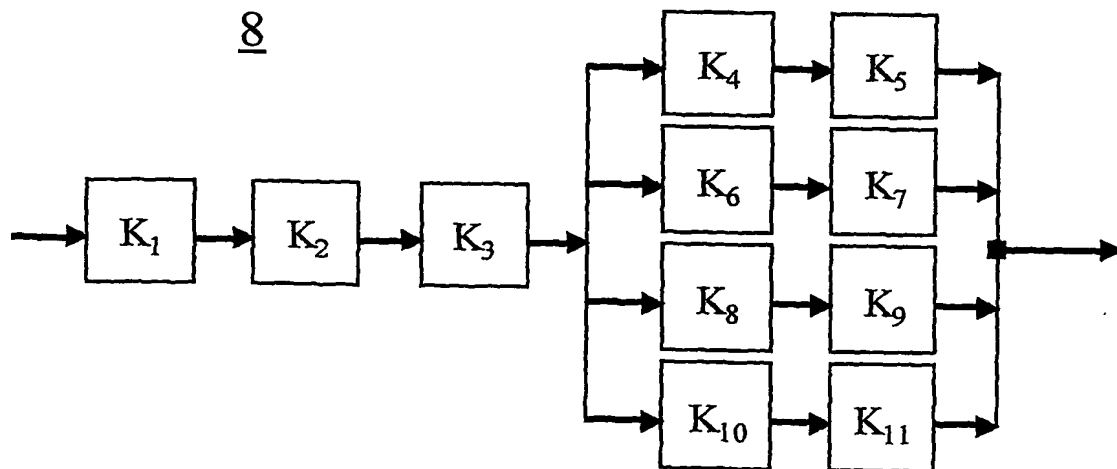


Fig. 2

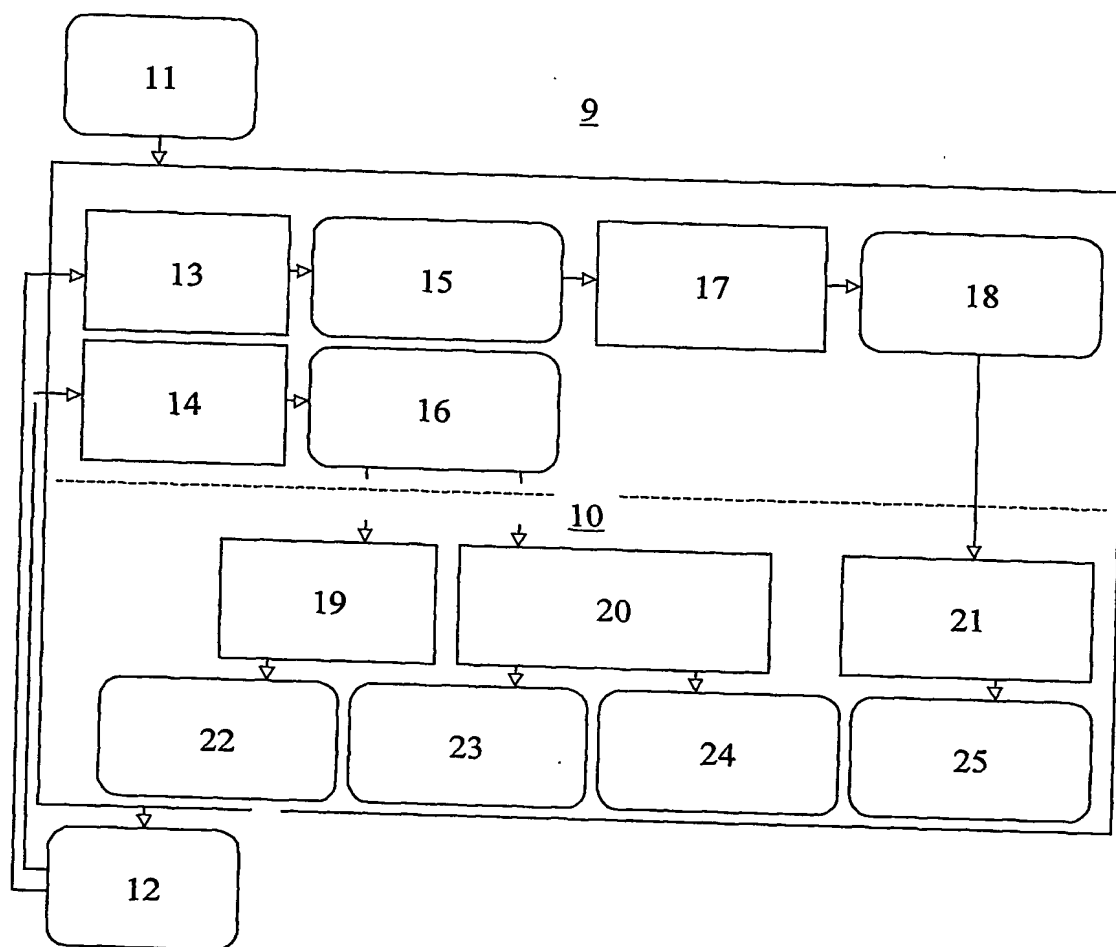


Fig. 3



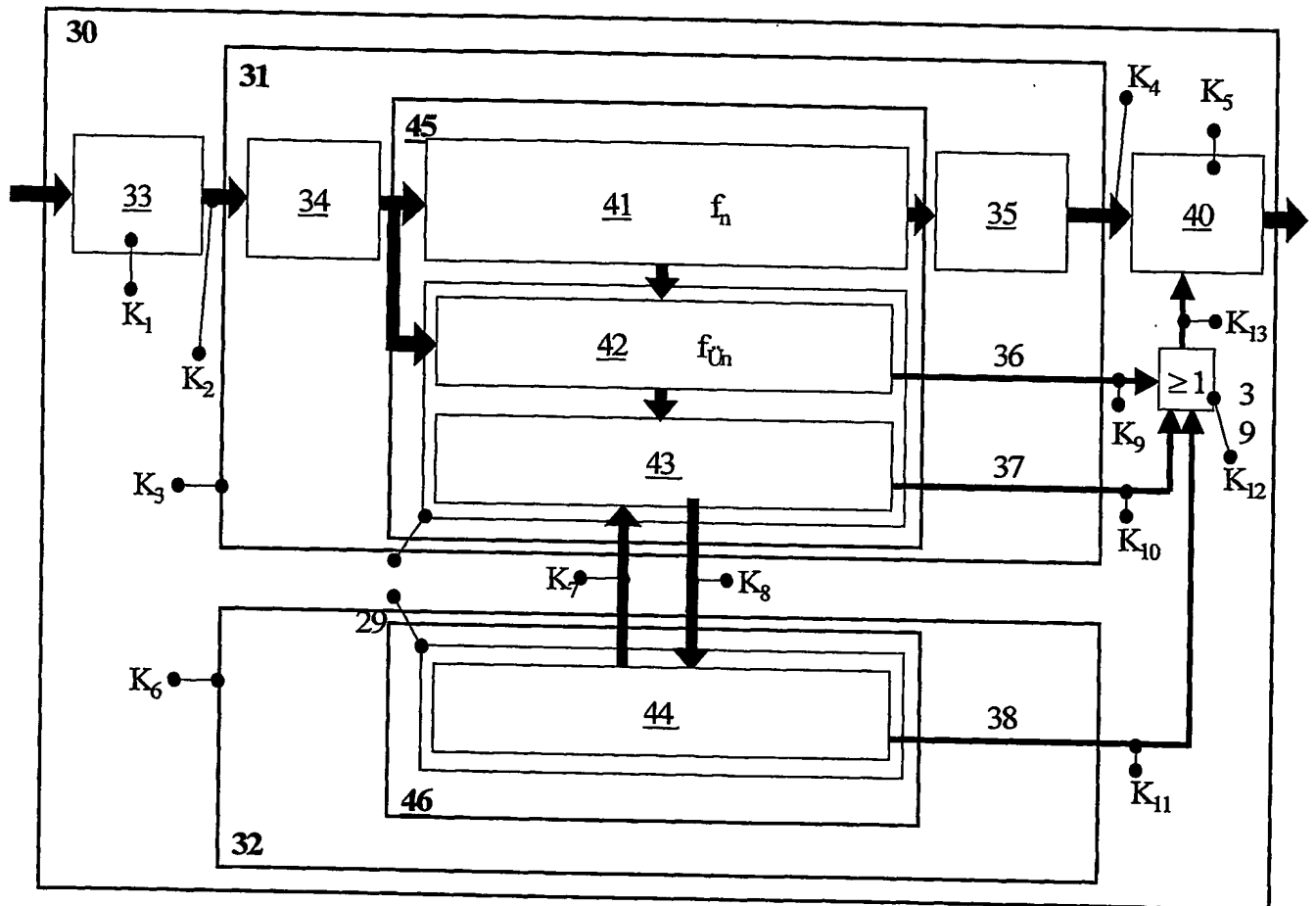
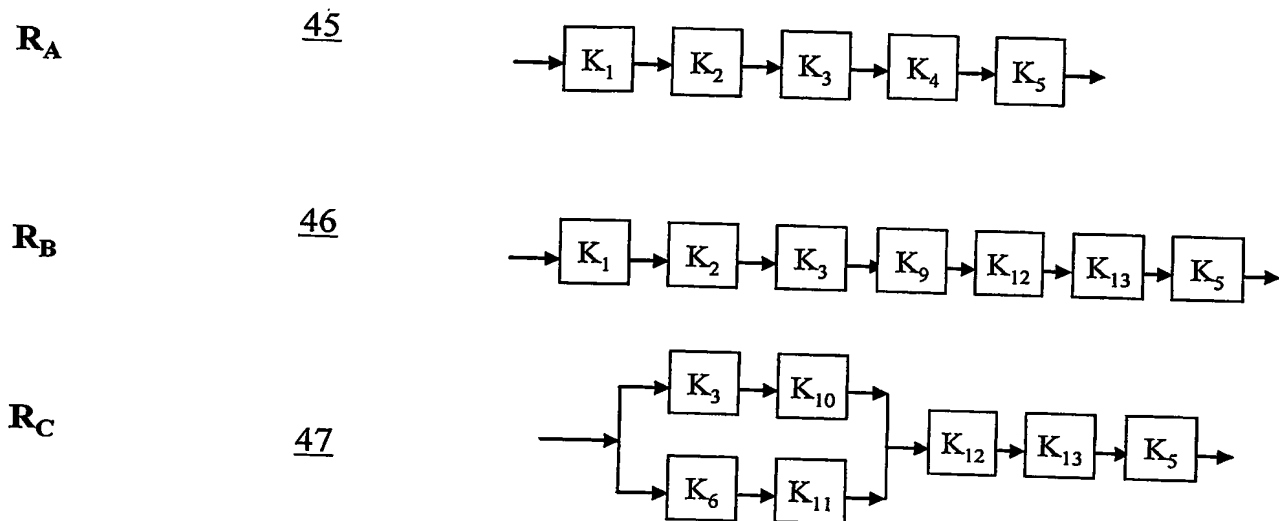


Fig. 4

**Fig. 5**